APPENDIX E

REDUNDANCY AS A DESIGN TECHNIQUE

E-1. Introduction to redundancy as a design technique

Redundancy can be defined as the existence of more than one means for accomplishing a given task. In general, all means must fail before there is a system failure. In chapter 2, we calculated the reliability of a redundant system. We will now provide a more detailed explanation of the calculations involved.

a. Simple parallel system. Consider the system with two parallel elements shown in figure E-1, with A having a reliability R_A and B having a reliability R_B. Define the probability of no failure as p and the probability of failure as q. Then p + q = 1 and the probability of system failure, Q, would be q_A q_B. (figure E-2 summarizes the characteristics of simple parallel active redundancy.)

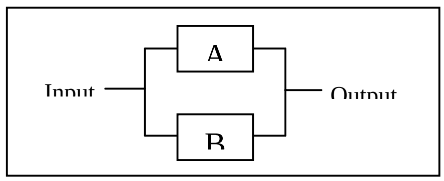
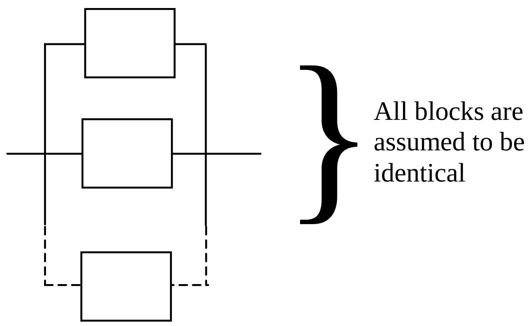
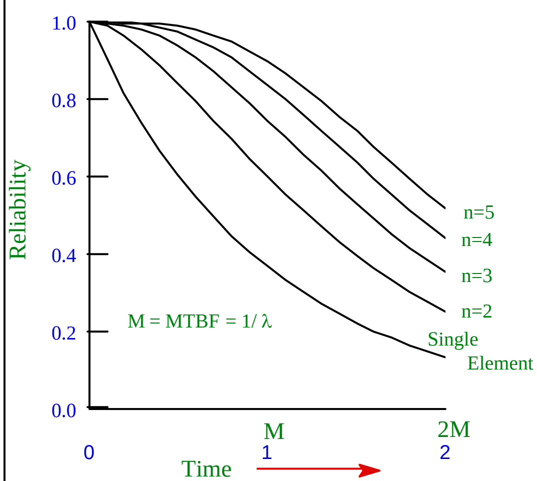


Figure E-1. Simple parallel network.





Reliability Function for Simple Parallel Reliability

APPLICATION

Provides protection against irreversible hardware failures for continuously operating equipments.

MATHEMATICAL MODEL

$R = 1 - (1 - e^{-\lambda t})^n$

APPROXIMATE MODEL

$R = 1 - (\lambda t)^n$ for small $\lambda t \leq 0.1$

where:

n	=	number of parallel elements
λ	=	failure rate
R	=	reliability

ADVANTAGES OF PARALLEL REDUNDANCY

- Simplicity
- Significant gain in reliability
- Applicable to both electronic (digital

DISADVANTAGES OF PARALLEL REDUNDANCY

- Load sharing must be considered
- Sensitive to voltage division across the elements
- Difficult to prevent failure propagation
- May present electronic circuit design problems

Figure E-2. Summary of simple parallel redundancy.

(1) Since reliability + unreliability = 1, the reliability, or probability of no failure, is given by $R = 1 - Q = 1 - q_A q_B$.

(2) If A has a reliability of 0.9 and B a reliability of 0.8, their unreliabilities q_A and q_B would be $q_A = 1 - 0.9 = 0.1$ and $q_B = 1 - 0.8 = 0.2$ and the probability of system failure would be $Q = (0.1)(0.2) = 0.02$. Hence the system reliability would be $R = 1 - Q = 0.98$, which is a higher reliability than either of the elements acting singly. Again, it should be pointed out that while redundancy reduces mission failures, it increases logistics failures.

(3) In general, with n elements in parallel, the overall probability of failure at time t is $Q(t) = q_1(t) \bullet q_2(t) \bullet \ldots \bullet q_n(t)$ and the probability of operating without failure is given by $R(t) = 1 - Q(t) = 1 - q_1(t) \bullet q_2(t) \bullet \ldots \bullet q_n(t)$. Because $q_i(t) = 1 - R_i(t)$ for each component, the latter equation can also be given as

$$R_{System}(t) = 1 - [1 - R_1(t)]\,[1 - R_2(t)] \ldots [1 - R_n(t)]$$

(4) When each of the component reliabilities is equal, the previous equations reduce to

$$Q(t) = [q(t)]^n$$

$$R_{System}(t) = 1 - [q(t)]^n = 1 - [1 - R(t)]^n$$

b. Interactions. So far it has been assumed that parallel components do not interact and that they are active all the time (or they may be activated when required by ideal failure sensing and switching devices). Needless to say, the latter assumption, in particular, is difficult to meet in practice. Therefore, the potential benefits of redundancy cannot be realized fully.

c. Basic formulas. Most cases of redundancy encountered will consist of various groupings of series and parallel elements. Figure E-3 typifies such system. The basic formulas previously given previously and in chapter 2 can be used to solve the overall system reliability R_S as equal to 0.938.

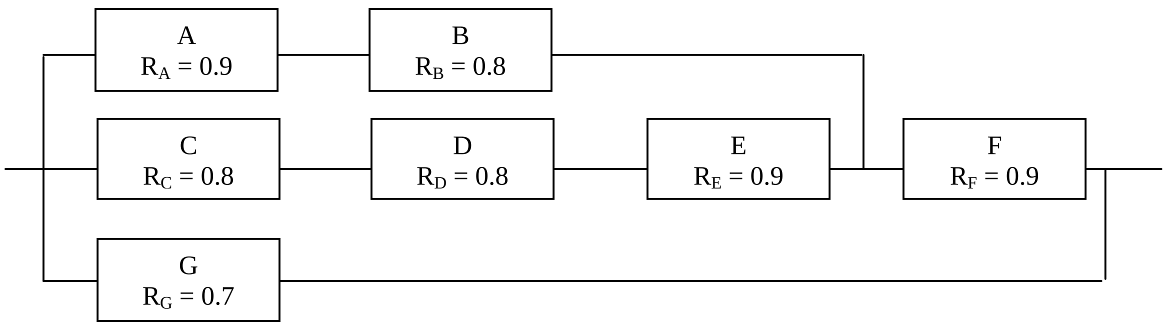


Figure E-3. Series-parallel redundancy system.

d. Levels of redundancy. Redundancy may be applied at the system level (essentially two systems in parallel) or at the subsystem, component, or part level within a system. Figure E-4 is a simplified reliability block diagram drawn to illustrate the several levels at which redundancy can be applied. System I is shown with its redundant alternative II, at the system level. II is in turn built up of redundant subsystems or components (B and C) and redundant parts within subsystems (b_1 and b_2 within subsystem B). From the reliability block diagram and a definition of block or system success, the paths that result in successful system operation can be determined. For example, the possible paths from input to output are [A, a, b_1, C_1], [A, a, b_1, C_2], [A, a, b_2, C_1], [A, a, b_2, C_2], and [I]. The success of each path may be computed by determining an assignable reliability value for each term and applying the multiplicative theorem. The computation of system success (all paths combined) requires a knowledge of the type of redundancy to be used in each case and an estimate of individual element reliability (or unreliability).

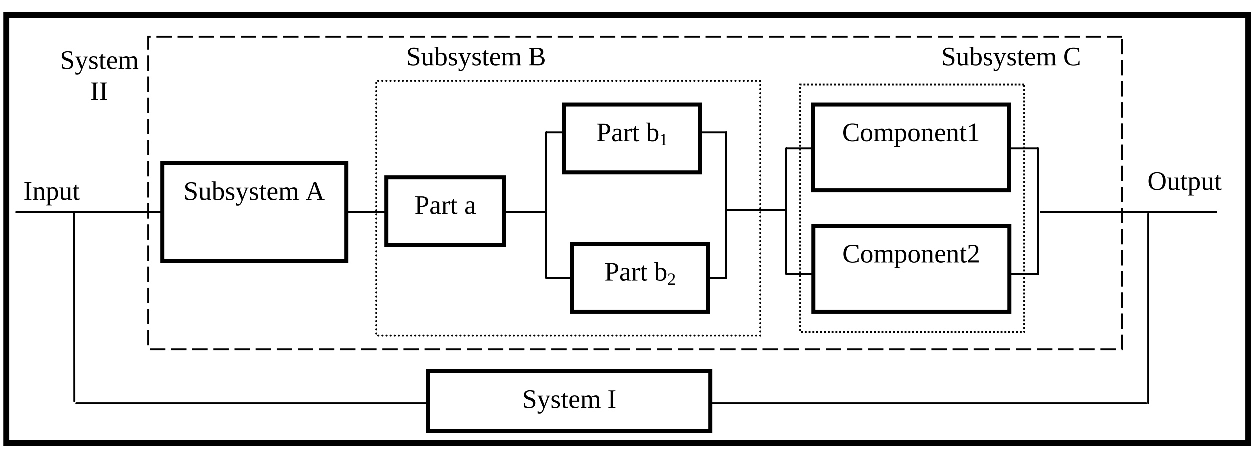


Figure E-4. Reliability block diagram depicting redundancy at the system, subsystem, component, and part levels.

e. Probability notation for redundancy computations. Reliability of redundancy combinations is expressed in probabilistic terms of success or failure -- for a given mission period, a given number of operating cycles, or a given number of time independent "events," as appropriate. The "MTBF" measure of reliability is not readily usable because of the non-exponential nature of the reliability function produced by redundancy. Reliability of redundancy combinations that are "time dependent" is therefore computed at a discrete point in time, as a probability of success for this discrete time period. The notation shown in figure E-5 is applicable to all cases and is used throughout this section.

R	=	probability of success or reliability of a unit or block
Q	=	$\overline{R}$ = probability of failure or unreliability of a unit or block
p	=	probability of success or reliability of an element
q	=	probability of failure or unreliability of an element

For probability statements concerning an event:

P(A)	=	probability that A occurs
$P(\overline{A})$	=	probability that A does not occur

For the probabilities:

$R + Q = 1$

$p + q = 1$

$P(A) + P(\overline{A}) = 1$

Figure E-5. Probability notation for redundancy computations.

f. Redundancy combinations. The method of handling redundancy combinations can be generalized as follows.

(1) Parallel elements, series units. If the elements are in parallel and the units in series (figure E-6), first evaluate the redundant elements to get the unit reliability. Then find the product of all unit reliabilities to obtain the block reliability. In the redundancy combination shown in figure E-6, Unit A has

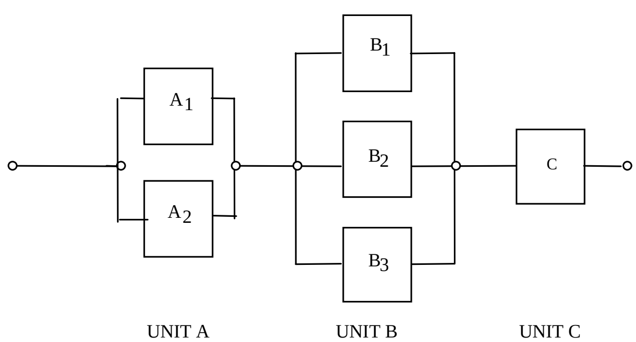


Figure E-6. Series-parallel configuration.

two parallel redundant elements, Unit B has three parallel redundant elements, and Unit C has only one element. Assume that all elements are independent. For Unit A to be successful, A_1 or A_2 must operate; for Unit B success, B_1, B_2 or B_3 must operate; and C must always be operating for block success. Translated into probability terms, the reliability of figure F-6 becomes:

$$R = \left[1 - P(\overline{A}_1 \bullet P(\overline{A}_2)\right] \bullet \left[1 - P(\overline{B}_1) \bullet P(\overline{B}_2) \bullet P(\overline{B}_3)\right] \bullet P(C)$$

If the probability of success, p, is the same for each element in a unit,

$$R = \left[1 - (1 - p_A)^2\right] \bullet \left[1 - (1 - p_B)^3\right] \bullet p_C$$
$$= (1 - q_A{}^2) \bullet (1 - q_B{}^3) \bullet P_C$$

where:

$$q_i = 1 - p_i$$

(2) *Series elements, parallel units*. If the elements are in series and the units or paths are in parallel (figure E-7), first obtain the path reliability by calculating the product of the reliabilities of all elements in each path. Then consider each path as a redundant unit to obtain the block reliability. Often there is a

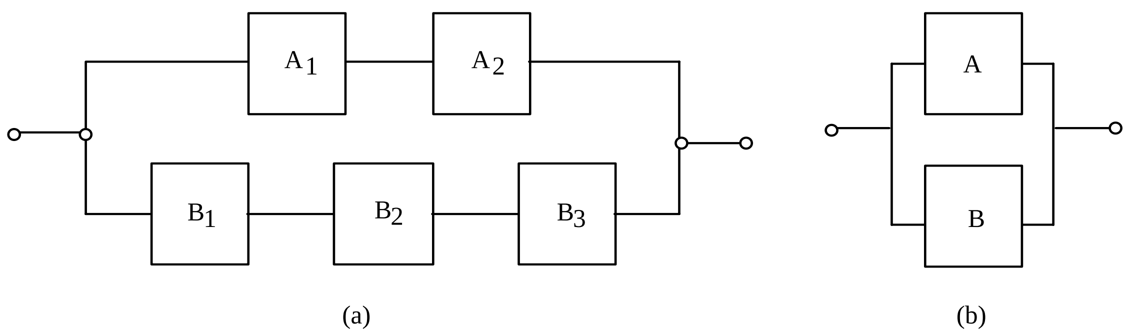


Figure E-7. Parallel-series configuration.

combination of series and parallel redundancy in a block as shown in figure E-7a. This arrangement can be converted into the simple parallel form shown in figure E-7b by first evaluating the series reliability of each path using the following equations (the terms on the right hand side represent element reliability):

$$p_A = p_{a_1} p_{a_2}$$

$$p_B = p_{b_1} p_{b_2} p_{b_3}$$

The block reliability can then be found from:

$$R = 1 - (1 - p_A) \bullet (1 - p_B)$$

$$= 1 - q_A q_B$$

g. Redundancy in time dependent situations. The reliability of elements used in redundant configurations is usually time dependent. If the relation between element reliability and time is known, inclusion of the time factor does not change the basic notation and approach to redundancy computation outlined above.

(1) Example of redundancy in time dependent situations. As an example, assume two active independent elements in parallel. System reliability is given by:

$$R = 1 - (1 - p_a)(1 - p_b) = 1 - 1 + p_a + p_b - p_a p_b$$

$$R = p_a + p_b - p_a p_b$$

(2) Expressing reliability over a period of time. The former equation is applicable for one time interval. To express reliability over a segment of time, the reliability of each element must be expressed as a function of time. Hence,

$$R(t) = p_a^{(t)} + p_b^{(t)} - p_a^{(t)}\, p_b^{(t)}$$

where:

$R(t)$ = system reliability for time t, $t > 0$

and $p_a^{(t)}, p_b^{(t)}$ = element reliabilities for time t

(3) When the exponential applies. The failure pattern of some components is described by the exponential distribution:

$$R(t) = e^{-\lambda t} = e^{-t/\theta}$$

where:

λ is the constant failure rate; t is the time interval over which reliability, R, is measured; and θ is the mean-time-between-failure.

(4) Two elements in series. For two elements in series with constant failure rates λ_a and λ_b, using the product rule of reliability gives:

$$R(t) = p_a^{(t)}\, p_b^{(t)} = e^{-\lambda_a t}\, e^{-\lambda_b t} = e^{-(\lambda_a + \lambda_b)t}$$

(5) System reliability function for redundant element systems. The system reliability, R(t), function for elements in series with constant failure rates is exponential. With redundant elements present in the system, however, the system reliability function is not itself exponential. This is illustrated by two operative parallel elements whose failure rates are constant. From:

$$R(t) = p_a + p_b - p_a p_b$$

$$R(t) = e^{-(\lambda_a)t} + e^{-(\lambda_b)t} - e^{-(\lambda_a + \lambda_b)t}$$

which is not of the simple exponential form $e^{-\lambda t}$. Element failure rates cannot, therefore, be combined in the usual manner to obtain the system failure rate if considerable redundancy is inherent in the design.

(6) MTBF of redundant systems. Although a single failure rate cannot be used for redundant systems with constant failure rate elements, the mean-time-to-failure of such systems can be evaluated. The mean life of a redundant "pair" whose failure rates are λ_a and λ_b, respectively, can be determined from:

$$MTBF = \int_o^{\infty} R(t)dt = \frac{1}{\lambda_a} + \frac{1}{\lambda_b} - \frac{1}{\lambda_a + \lambda_b}$$

or, if the failure rates of both elements are equal,

$$R(t) = 2e^{-\lambda t} - e^{-2\lambda t}$$

and

$$MBTF = \frac{3}{2\lambda} = \frac{3}{2}\theta$$

(7) Three elements in parallel. For three independent elements in parallel, the reliability function is:

$$R(t) = 1 - \left[(1 - e^{-\lambda_a t})(1 - e^{-\lambda_b t})(1 - e^{-\lambda_c t})\right]$$

and

$$MTBF = \frac{1}{\lambda_a} + \frac{1}{\lambda_b} + \frac{1}{\lambda_c} - \frac{1}{\lambda_a + \lambda_b} - \frac{1}{\lambda_a + \lambda_c} -$$

$$\frac{1}{\lambda_b - \lambda_c} + \frac{1}{\lambda_a + \lambda_b + \lambda_c}$$

(8) Reliability function for three elements in parallel. For three independent elements in parallel when $\lambda_a = \lambda_b = \lambda_c = \lambda$, the reliability function is:

$$R(t) = 3e^{-\lambda t} - 3e^{-2\lambda t} + e^{-\lambda t}$$

and

$$MTBF = \frac{3}{\lambda} - \frac{3}{2\lambda} + \frac{1}{3\lambda} = \frac{1}{\lambda} + \frac{1}{2\lambda} + \frac{1}{3\lambda} = \frac{11}{6\lambda} = \frac{11}{6}\theta$$

(9) General rule. In general, for n active parallel elements, each element having the same constant failure rate, λ,

$$R(t) = 1 - \left(1 - e^{-\lambda t}\right)^n$$

and

$$\text{MTBF} = \sum_{i=1}^{n} \frac{1}{i\lambda} = \sum_{i=1}^{n} \frac{\theta}{i}$$

h. Types of redundancy. There are two basic types of redundancy: active and standby.

(1) Active redundancy. External components are not required to perform the function of detection, decision and switching when an element or path in the structure fails. The redundant units are always operating and automatically pick up the load for a failed unit. An example is a multiengine aircraft. The aircraft can continue to fly with one or more engines out of operation.

(2) Standby redundancy. External elements are required to detect, make a decision and switch to another element or path as a replacement for a failed element or path. Standby units can be operating (e.g., a redundant radar transmitter feeding a dummy load is switched into the antenna when the main transmitter fails) or inactive (e.g., a backup generator is turned on when the primary power source fails).

(3) Other forms of redundancy. Table E-1 summarizes a variety of redundancy techniques. The most important of these are discussed later in this appendix.

Table E-1. *Redundancy techniques*

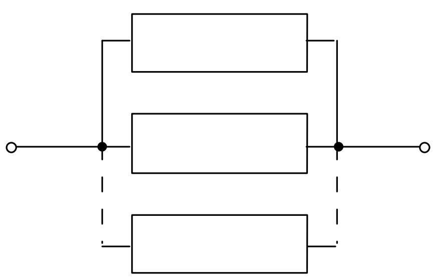
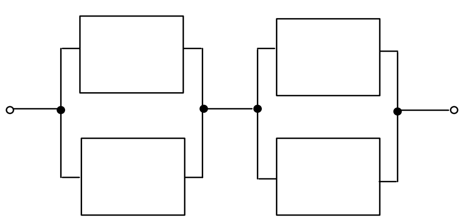
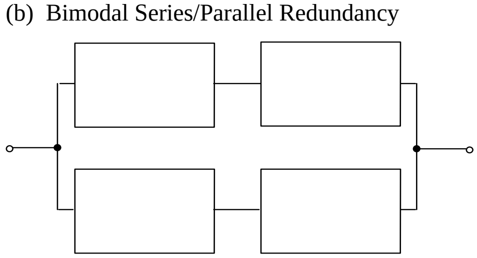
<u>Simple Parallel Redundancy (Active Redundancy)</u> 	In its simplest form, redundancy consists of a simple parallel combination of elements. If any element fails open, identical paths exist through parallel redundant elements.
(a) Bimodal Parallel/Series Redundancy  (b) Bimodal Series/Parallel Redundancy 	A series connection of parallel redundant elements provides protection against electrical shorts and opens. Direct short across the network due to a single element shorting is prevented by a redundant element in series. An open across the network is prevented by the parallel element. Network (a) is useful when the primary element failure mode is open. Network (b) is useful when the primary element failure mode is short.

Table E-1. Redundancy techniques (Cont'd)

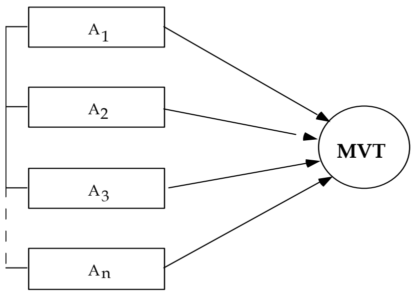
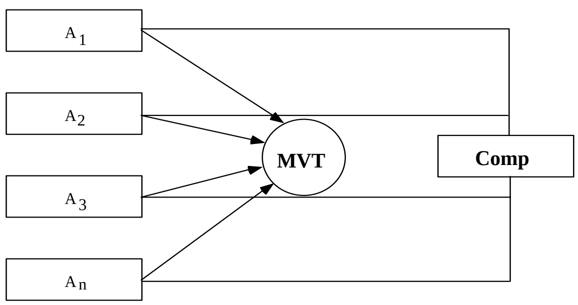
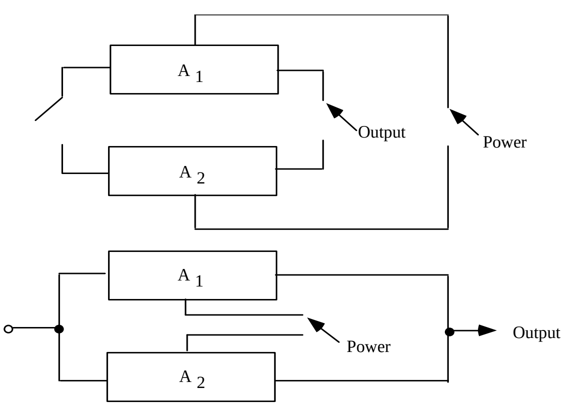
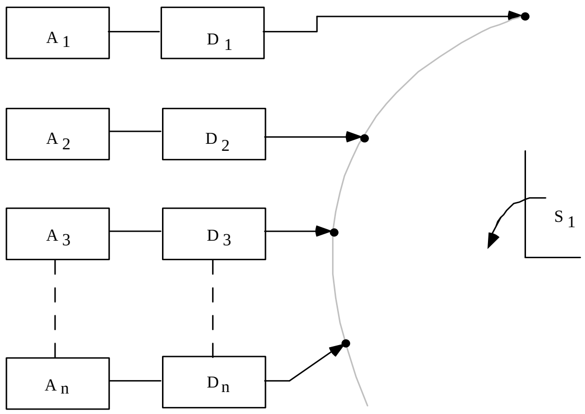
Majority Voting Redundancy  	Decision can be built into the basic parallel redundant model by inputting signals from parallel elements into a voter to compare each element's signal with the signals of the other elements. Valid decisions are made only if the number of useful elements exceeds the failed elements.
Adaptive Majority Logic  	This technique exemplifies the majority logic configuration discussed previously with a comparator and switching network to switch out or inhibit failed redundant elements.
Standby Redundancy  	A particular redundant element of a parallel configuration can be switched into an active circuit by connecting outputs of each element to switch poles. Two switching configurations are possible. The elements may be isolated by the switch until switching is completed and power applied to the element in the switching operation. All redundant elements are continuously connected to the circuit and a single redundant element activated by switching power to it.

Table E-1. Redundancy techniques (Cont'd)

<table>
<tr><td>Operating Standby Redundancy

</td><td>In this application, all redundant units operate simultaneously. A sensor on each unit detects failures. When a unit fails, a switch at the output transfers to the next unit and remains there until failure.</td></tr>
</table>

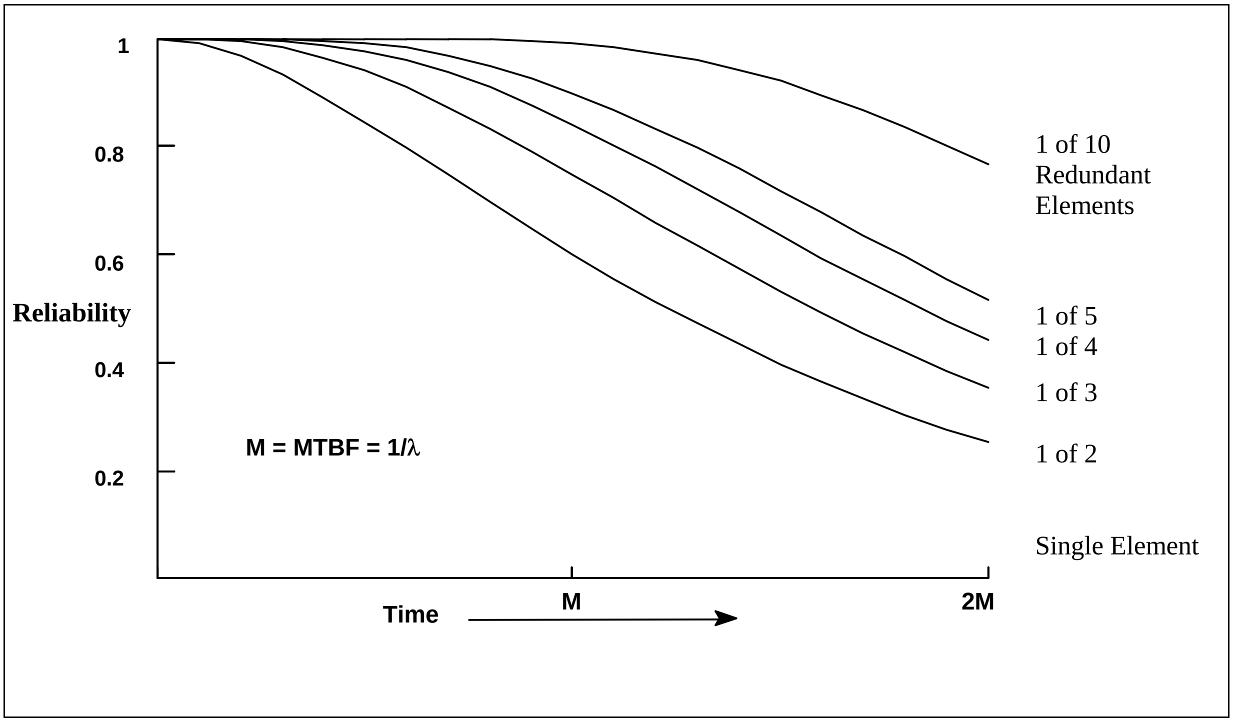
i. Limited benefits of redundancy. In general, the reliability gain for additional redundant elements decreases rapidly for additions beyond a few parallel elements. As illustrated by figure E-8 for simple parallel redundancy, there is a diminishing gain in reliability and MTBF as the number of redundant elements is increased. As shown for the simple parallel case, the greatest gain achieved through addition of the first redundant element is equivalent to a 50% increase in the system MTBF.

(1) Redundancy may not help. The reliability of certain redundant configurations may actually be less than that of a single element due to the serial reliability of switching or other peripheral devices needed to implement the particular redundancy configuration. Care must be exercised to ensure that reliability gains are not offset by increased failure rates due to switching devices, error detectors and other peripheral devices needed to implement the redundancy.

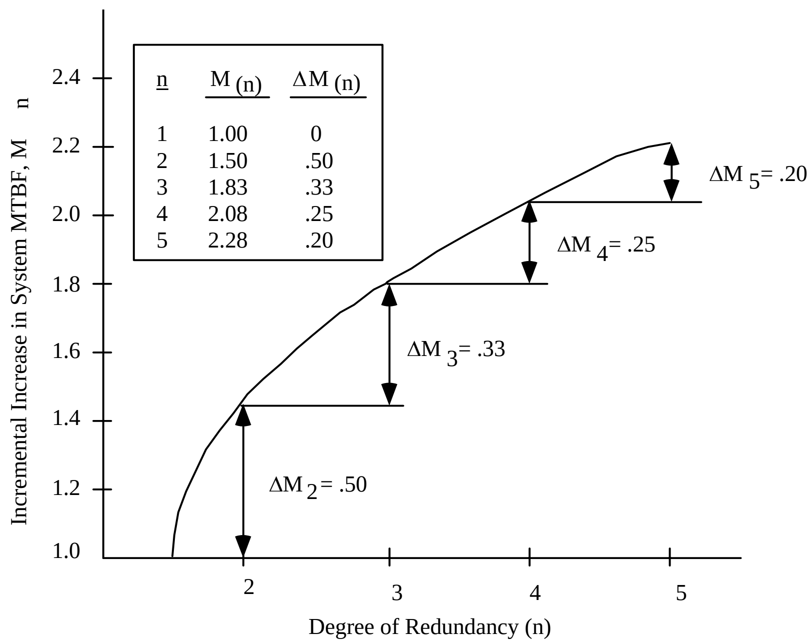
(2) Increasing the effectiveness of redundancy. The effectiveness of certain redundancy techniques (especially standby) can be enhanced by repair. Standby redundancy allows repair of the failed unit (while operation of the good unit continues uninterrupted) by virtue of the switching function built into the standby redundant configuration. Through continuous or interval monitoring, the switchover function can provide an indication that failure has occurred and operation is continuing on the alternate channel. With a positive failure indication, delays in repair are minimized. A further advantage of switching is related to built-in test (BIT) objectives. Built-in test can be readily incorporated into a sensing and switchover network for ease of maintenance purposes.

(3) An example. An illustration of the enhancement of redundancy with repair is shown in figure E-9. The increased reliability brought about by incorporation of redundancy is dependent on effective isolation of redundant elements. Isolation is necessary to prevent failure effects from adversely affecting other parts of the redundant network. In some cases, fuses or circuit breakers, overload relays, etc., may be used to protect the redundant configuration. These items protect a configuration from secondary effects of an item's failure so that system operation continues after the element failure. The susceptibility of a particular redundant design to failure propagation may be assessed by using an FMEA. The

particular techniques addressed there offer an effective method of identifying likely fault propagation paths.



a. Simple active redundancy where one of n elements is required.



b. Incremental increase in system MTBF for n active elements.

Figure E-8. The gain in reliability decreases as the number of active elements increases.

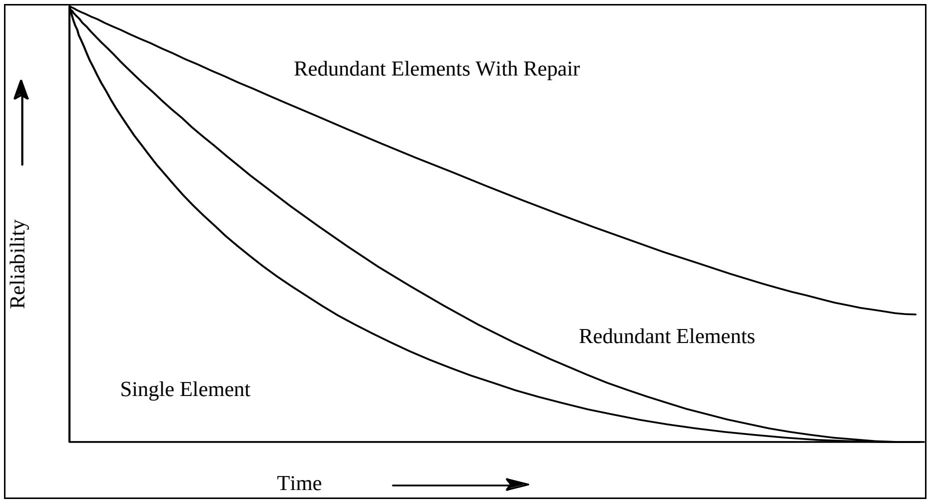


Figure E-9. Reliability gain for repair of simple parallel element at failure.

j. Redundancy in protective circuits. Redundancy may be incorporated into protective circuits[1] as well as the functional circuit that it protects. Operative redundancy configurations of protection devices (e.g., fuse, circuit breaker) can be used to reduce the possibility that the "protected" circuit is not completely disabled should the protective circuit device open prematurely or fail to open due to overcurrent.

k. Checking status of redundancy. The incorporation of redundancy into a design must take into account "checkability." Some items may not be checkable prior to mission start. Such items must then be assumed to be functional at the beginning of the mission. In reality, pre-mission failures of redundant items could be masked. If it is not known that redundant elements are operational prior to mission start, then the purpose of redundancy can be defeated because the possibility exists of starting a mission without the designed redundancy (a reliability loss). The designer must take this into account for built-in test planning, inclusion of test points, packaging, etc., when redundancy is used in system design.

l. k of N (Partial) Redundancy. Instances in which the system is successful if at least one of n parallel paths is successful have been discussed. In other instances, at least k out of n elements must be successful. In such cases, the reliability of the redundant group (each with the same probability of success, p) is given by a series of additive binomial terms in the following form.

$$P(k, n \mid p) = \binom{n}{k} p^k (1-p)^{n-k}$$

(1) Partial redundancy example 1. A generator has three filters. The generator will operate if at least two filters are operational, that is, if k = 2 or k = 3. The probability of each channel being successful is equal to p; then

$$R = P(2, 3 \mid p) + P(3, 3 \mid p)$$

$$R = \binom{3}{2} p^2 (1-p) + \binom{3}{3} p^3 (1-p)^0$$

[1] It should be noted that the need for or usefulness of modeling reliability at the circuit level is not universally accepted. In particular, many engineers question the value of such modeling for modern technologies. Discussion of circuit-level modeling is included here since it may be of value in some instances.

$$R = 3p^2\ (1 - p) + p^3$$

$$R = 3p^2 - 2p^3$$

(2) Partial redundancy example 2. Use of the binomial formula becomes impractical for hand calculation in multi-element partial redundant configurations when the values of n and k become large.[2] In these cases, the normal approximation to the binomial may be used. The approach can be best illustrated by an example. A transmitting array is designed using 1000 RF elements to achieve design goal performance for power output and beam width. A design margin has been provided, however, to permit a 10% loss of RF elements before system performance becomes degraded below the acceptable minimum level. Each element is known to have a failure rate of 1000 x 10^{-6} failures per hour. The proposed design is illustrated in figure E-10, where the total number of elements is n = 1000; the number of elements required for system success is k = 900; and, the number of element failures permitted is r = 100. It is desired to compute and plot the reliability function for the array.

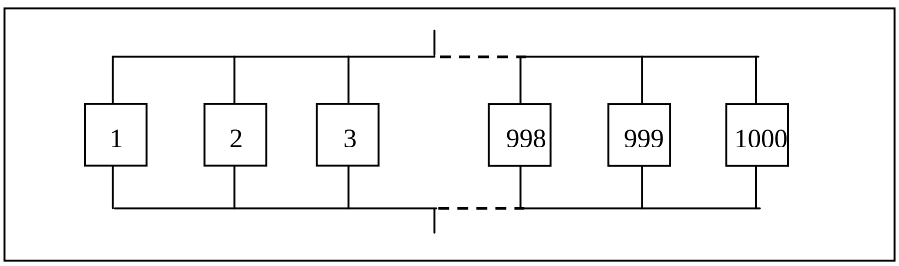


Figure E-10. Partial redundant array.

(a) For each discrete point of time, t, the system reliability function, $R_s t$ is given by the binomial summation as:

$$R_s t = \sum_{x=0}^{r} \binom{n}{x} p^{n-x} q^x$$

$$= \sum_{x=0}^{100} \binom{1000}{x} \left(e^{-\lambda t}\right)^{n-x} \left(1 - e^{-\lambda t}\right)^x$$

where:

$q = 1 - e^{-\lambda t}$

$p = e^{-\lambda t}$

x = number of failures

λ = element failure rate

(b) The binomial summation can be approximated by the standard normal distribution function using table E-2 to compute reliability for the normalized statistic z.

[2] See any good textbook on probability and statistics.

Table E-2. Reliability calculations for example 2

Time, t	z	$F(z) = R_s(t)$
90	1.570	0.9420
95	0.989	0.8389
105	0.000	0.5000
110	-0.420	0.3370
120	-1.300	0.0970
130	-2.030	0.0210

Note that $R_s(t) = F(z)$

where:

$$z = \frac{x - \mu}{\sigma} = \frac{x - nq}{\sqrt{npq}} = \frac{x - n(1 - e^{-\lambda t})}{\sqrt{n(1 - e^{-\lambda t})e^{-\lambda t}}}$$

(c) By observation, it can be reasoned that system MTBF will be approximately 100 hours, since 100 element failures are permitted and one element fails each hour of system operation. A preliminary selection of discrete points at which to compute reliability might then fall in the 80- to 100-hour bracket. Table E-3 shows the calculations.

Table E-3. MTBF calculations for example 2

At 80 Hours:

$$q = 1 - e^{-\lambda t} = 1 - e^{-(1000 \bullet 10^{-6} \bullet 80)} = 0.077$$

$$p = e^{-(1000 \bullet 10^{-6} \bullet 80)} = 0.923$$

$$\mu = nq = 1000\,(1 - e^{-(1000 \bullet 10^{-6} \bullet 80)}) = 77$$

$$\sigma = \sqrt{npq} = \sqrt{1000(0.077)(0.923)} = \sqrt{71.07} = 8.4$$

x = 100

$$z_{80} = \frac{100 - 77}{8.4} = 2.74$$

$R_s(80) = F(z_{80}) = F(+2.74) = 0.997$, from standard normal tables

At 100 Hours:

$$\mu = nq = 1000\,(1 - e^{-1000 \bullet 10^{-6} \bullet 100}) = 95$$

$$p = e^{-1000 \bullet 10^{-6} \bullet 100} = 0.905$$

$$\sigma = \sqrt{npq} = \sqrt{86} = 9.3$$

x = 100

$$z_{100} = \frac{100 - 9.5}{9.3} = 0.54$$

$$R_s(100) = F(z_{100}) = F(+0.54) = 0.705$$

These points are then used to plot the reliability function for the array, shown in Figure E-11. Also shown in the figure are curves for r = 0, 50, and 150.

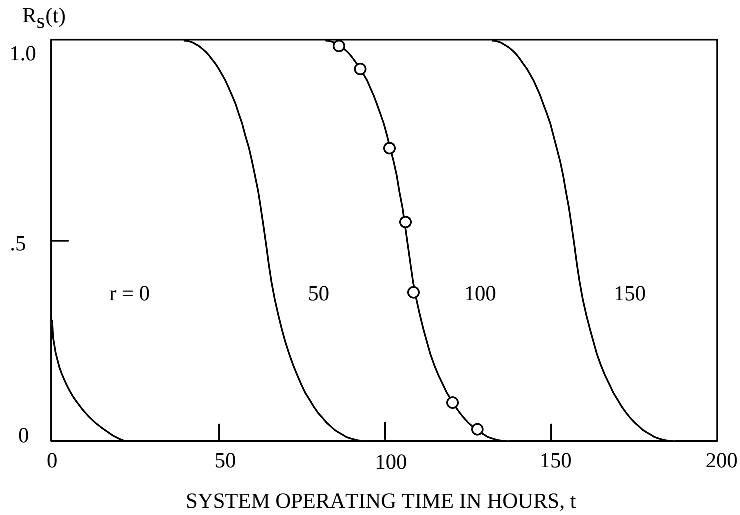


Figure E-11. Reliability functions for partial redundant array of figure E-10.

m. Operating standby redundancy. Until now we have assumed that switching devices were either absent or failure free. We now deal with cases whose redundant elements are continuously energized but do not become part of the system until switched in after a primary element fails. We will consider two modes of failure that can be associated with the switching mechanism: Type 1 - The switch may fail to operate when it is supposed to; and Type 2 - The switch may operate without command (prematurely). In the discussions that follow, q_s = probability of a Type 1 failure, and q'_s = probability of a Type 2 failure. Note that the probability of switching failures must be considered in modeling redundancy with switching. The consideration of such failures can be complex. If the switching reliability is high in comparison with element reliability (i.e., switch failure rate is one-tenth that of the element failure rate), it is often possible to simplify the model with an acceptable loss of accuracy by ignoring switch failures.

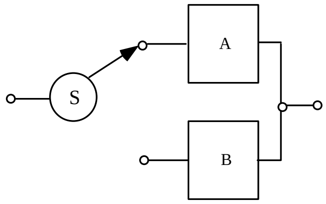
(1) Two parallel elements. Consider the system in figure E-12. There are three possible states that could lead to system failure. In state 1, A fails, B succeeds, and the switch fails (Type 1 failure). In state 2, A succeeds, B fails, and the switch fails (Type 2 failure). In state 3, A fails and B fails. The calculations for the system reliability are shown in the figure.

(2) Three Parallel Elements. Figure E-13 illustrates this type circuit. It operates as follows: If A fails, S switches to B. If B then fails, S switches to C. Enumerating all possible switching failures shows two kinds of Type (1) failure and four kinds of Type (2) failure as shown in the figure.

n. Voting Redundancy. Figure E-14 shows three elements, A, B, and C, and the associated switching and comparator circuit which make up a voting redundant system. The circuit function will always be performed by an element whose output agrees with the output of at least one of the other elements. At least two good elements are required for successful operation of the circuit. Two switches are provided so that a comparison of any two outputs of the three elements can be made. A comparator circuit is required that will operate the two switches so that a position is located where the outputs again agree after one element fails.

(1) Perfect switching and comparison. If comparison and switching are failure free, the system will be successful as long as two or three elements are successful. In this case,

$$R = p_a p_b + p_a p_c + p_b p_c - 2p_a p_b p_c$$



The unreliability of the system, Q, is

$$Q = p_a \; p_q \; q'_s + q_a \; p_b \; q_s + q_a \; q_b$$

The reliability of the system, R, is

$$R = 1 - Q = 1 - (p_a \; p_q \; q'_s + q_a \; p_b \; q_s + q_a \; q_b)$$

Example: Assume

$$q_a = q_b = 0.2 \text{ and } q_s = q'_s = 0.1$$

Then

$$Q = p_a \; p_q \; q'_s + q_a \; p_b \; q_s + q_a \; q_b$$

$$= (0.8)(0.2)(0.1) + (0.2)(0.8)(0.1) + (0.2)(0.2) = 0.072$$

$$R = 1 – Q = 1 - 0.072 = 0.928$$

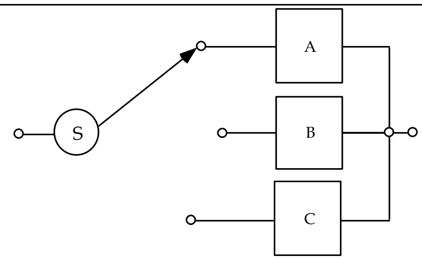
If we are not concerned with Type (2) failures, $q'_s = 0$, and the unreliability is

$$Q = q_a \; p_b \; q_s + q_a \; q_b$$

$$= (0.2)(0.8)(0.1) + (0.2)(0.2) = 0.056$$

$$R = 1 - 0.056 = 0.944$$

Figure E-12. Redundancy with switching.



Type (1) Switching Failures:

- q_{s_1} - A fails, S does not switch to B.
- q_{s_2} - A fails, S switches to B, B fails, S fails to switch to C.

Type (2) Switching Failures:

- q'_{s_3} - A succeeds, but S switches to B.
- q'_{s_4} - A succeeds, S switches to B, B fails, S does not switch to C.
- q'_{s_5} - A succeeds, S switches to B, B succeeds, S switches to C.
- q'_{s_6} - A fails, S switches to B, B succeeds, S switches to C.

Figure E-13. Three-element redundant configuration with switching.

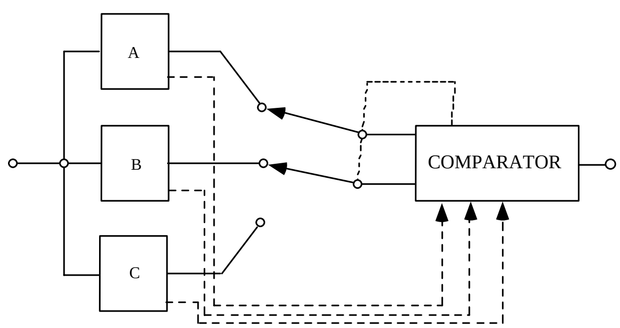


Figure E-14. Three-element voting redundancy.

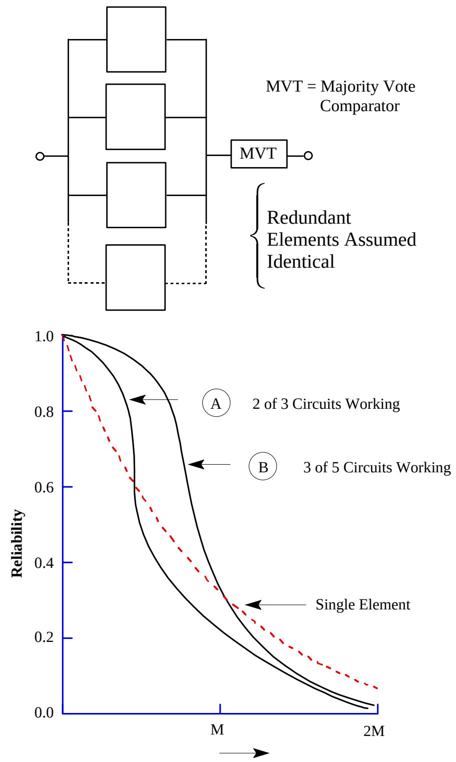
(2) Imperfect switching. If failure free switching cannot be assumed, conditional probabilities of switching operation have to be considered. To simplify the discussion, consider the probability of the comparator and switches failing in such a manner that the switches remain in their original positions. If this probability is q_s, then

$$R = p_a\ p_b + (p_a\ p_c + p_b\ p_c - 2p_a\ p_b\ p_c)(1 - q_s)$$

(3) Example. Here is an example of a voting redundant system (information and expressions for the general majority voting case are given in figure E-15). Let all three elements have the same probability of success, 0.9, i.e., $p_a = p_b = p_c = 0.9$. Assume that the comparator switch has a probability of failing (q_s) of 0.01.

$$R = 9^2 + \left[0.9^2 + 0.9^2 - 2(0.9)^3\right]\left[1 - 0.01\right]$$

$$R = 970$$



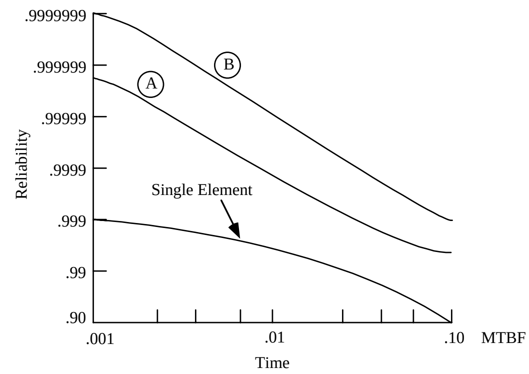
Reliability Function for Majority Voting Redundancy

ADVANTAGES

- Can be implemented to provide indication of defective elements
- Can provide a significant gain in reliability for short mission times (less than one MTBF)

DISADVANTAGES

- Requires voter reliability be significantly better than that of element
- Lower reliability for long mission time (greater than one MTBF)



Reliability For Mission Time Less Than One MTBF

APPLICATION

Generally used with logic circuitry for either continuous or intermittent operation. This technique with minor modification, may be put in the form of adaptive majority logic or gate connector redundancy

MATHEMATICAL MODEL

$$R = \left[\sum_{i=0}^{n} \binom{2n+1}{i} \left(1 - e^{-\lambda t}\right) e^{-\lambda t(2n+1-i)}\right] e^{-\lambda_m t}$$

Figure E-15. Majority voting redundancy.

o. Inactive standby redundancy. In a system with redundant elements on an inactive standby basis (not energized), no time is accumulated on a secondary element until a primary element fails. For a two-element system, the reliability function can be found directly as follows. The system will be successful at time t if either of the following two conditions holds (let A be the primary element): A is successful up to time t. or A fails at time $t_1 < t$, and B operates from t_1 to t.

(1) The exponential case. For the exponential case where the element failure rates are λ_a and λ_b, the reliability of the standby pair is given by the following equation.

$$R(t) = \frac{\lambda_b}{\lambda_b - \lambda_a} e^{-\lambda_a t} - \frac{\lambda_a}{\lambda_b - \lambda_a} e^{-\lambda_b t}$$

(This is a form of the mixed exponential and it does not matter whether the more reliable element is used as the primary or as the standby element.)

(2) MTBF. The mean-time-to-failure of the system just described is

$$MTBF = \frac{\lambda_a + \lambda_b}{\lambda_a \lambda_b}$$

$$\theta_a + \theta_b$$

$$= 2\theta, \text{ when } \theta_a = \theta_b = \theta$$

(3) Multiple elements. For n elements of equal reliability, it can be shown that,

$$R(t) = e^{-\lambda t} \sum_{r=0}^{n-1} \frac{(\lambda t)^r}{r!}$$

where:

r is the number of failures

$$MTBF = \frac{n}{\lambda} = n\theta$$

(4) Inactive standby redundancy as a function of mission time. Figure E-16 is a chart relating system reliability to the reliability of individual operating standby redundant parallel elements as a function of mission time, t/θ. By entering the chart at the time period of interest and proceeding vertically to the allocated reliability requirement, the required number of standby elements can be determined.

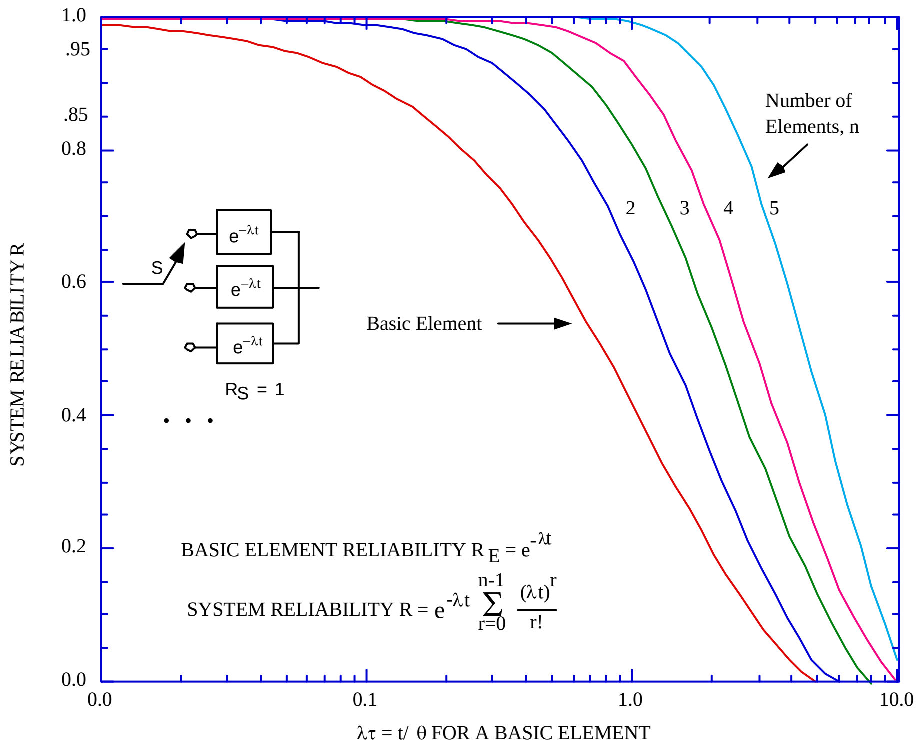


Figure E-16. System reliability for n standby redundant elements.

(5) Example of inactive standby redundancy. A critical element within a system has a demonstrated MTBF, θ = 100 hours. A design requirement has been allocated to the function performed by this element of R_s = 0.98 at 100 hours. This corresponds to a 30-to-1 reduction in unreliability compared with that which can be achieved by a single element. In this case, n = 4 will satisfy the design requirement at $t/\theta = 1$. In other words, a four-element standby redundant configuration would satisfy the requirement. Failure rates of switching devices must next be taken into account.

p. Dependent failure probabilities. Up to this point, it has been assumed that the failure of an operative redundant element has no effect on the failure rates of the remaining elements. Dependent failures might occur, for example, with a system having two elements in parallel where both elements share the full load.

(1) Conditional events. Figure E-17 illustrates an example of conditional or dependent events. Assume elements A and B are both fully energized, and normally share or carry half the load, L/2. If either A or B fails, the survivor must carry the full load, L. Hence, the probability that one fails is dependent on the state of the other, if failure probability is related to load or stress. The system is operating satisfactorily at time t if either A or B or both are operating successfully.

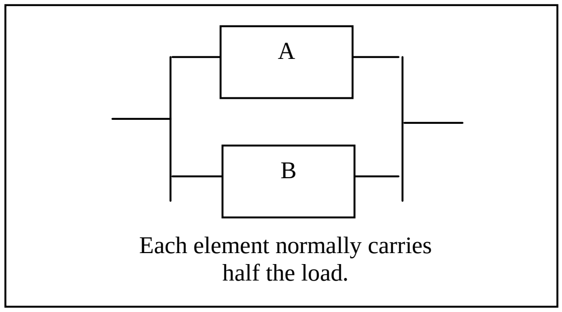


Figure E-17. Load sharing redundant configuration.

(a) Figure E-18 illustrates the three possible ways the system can be successful. The bar above a letter represents a failure of that element. A primed letter represents operation of that element under full load; absence of a prime represents operation under half load. If the elements' failure times are exponentially distributed and each has a mean life of θ under load L/2 and $\theta' = \theta/k$ under load L where $k \geq 0$, block reliability and system mean life are given by:

$$R(t) = \frac{2\theta'}{2\theta' - \theta} e^{-t/\theta'} - \frac{\theta}{2\theta' - \theta} e^{-2t/\theta}$$

$$\theta = \theta/k + \theta/2$$

(b) When k = 1, the system is one in which load sharing is not present or an increased load does not affect the element failure probability. Thus, for this case, θ_s s is equal to $3\theta/2$.

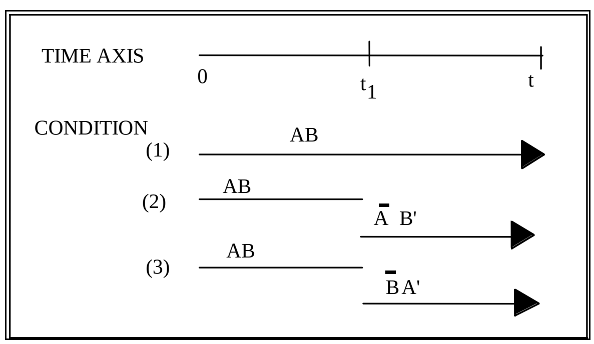


Figure E-18. Success combinations in two-element load-sharing case.

q. Optimum allocation of redundancy. Decision and switching devices may fail to switch when required or may operate inadvertently. However, these devices are usually necessary for redundancy, and increasing the number of redundant elements increases the number of switching devices. If such devices are completely reliable, redundancy is most effective at lower system levels. If switching devices are not failure free, the problem of increasing system reliability through redundancy becomes one of choosing an optimum level at which to replicate elements.

(1) Redundancy is not free. Since cost, weight, and complexity factors are always involved, the minimum amount of redundancy that will produce the desired reliability should be used. Thus efforts should be concentrated on those parts of the system that are the major causes of system unreliability.

(2) Example. Assume that we have two elements, A and B, with reliabilities over a certain time period of 0.95 and 0.50, respectively. If A and B are joined to form a series non-redundant circuit, its reliability is

$$R = (0.95)(0.50) = 0.475$$

(a) If we duplicate each element, as in figure E-19a,

$$R_1 = [1 - (0.50)^2]\,[1 - (0.05)^2] = 0.748$$

(b) Duplicating element B only, as in figure E-19b,

$$R_2 = 0.95\ [1 - (0.50)^2] = 0.712$$

(c) Obviously, duplicating element A contributes little to increasing reliability. Triplication of B gives the configuration shown in figure E-19c and $R_3 = 0.95\ [1 - (0.5)^3] = 0.831$, which is a 75% increase in the original circuit reliability as compared to the 58% increase of R_1.

(d) If complexity is the limiting factor, duplicating systems is generally preferred to duplicating elements, especially if switching devices are necessary. If another series path is added in parallel, we have the configuration in figure E-19d, and $R_4 = 1 - (1 - 0.475)^4 = 0.724$, which is only slightly less than R_1. If switches are necessary for each redundant element, R_4 may be the best configuration. A careful analysis of the effect of each element and switch on system reliability is a necessary prerequisite for proper redundancy application.

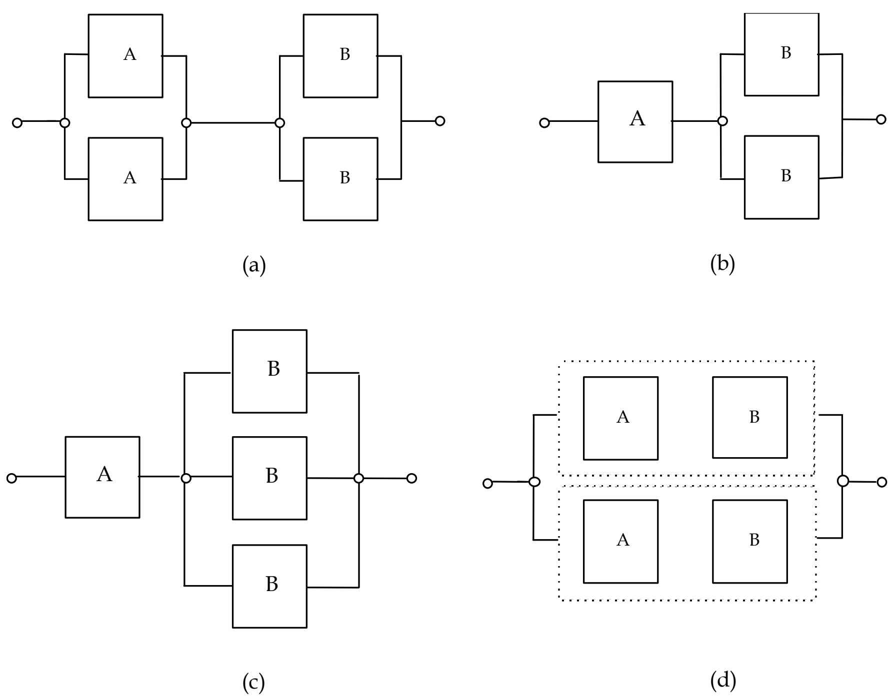


Figure E-19. Possible alternative redundant configurations for optimization example. Baseline is a series system with two elements, A and B.